Kerberos

Functions vulnerable to TOCTOU issues

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 7425 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Indeterminate File/Path • TOCTOU - Time of Check, Time of Use
Software Context	• Authorization
Location	• kerberos/krb.h
Description	The krb_recvauth() function reads a ticket/ authenticator pair from the indicated socket. The argument list includes a filename argument which specifies the filename which the service program should use to obtain the secret key(s) for the service. If you set this argument to "", krb_recvauth() looks for the service key in the file /etc/srvtab. krb_set_tkt_string() sets the name of the file that holds the user's cache of Kerberos server tickets and associated session keys. The string filename passed in is copied into local storage. Only MAXPATHLEN-1 characters of the filename are copied in for use as the cache file name. This routine should be called during initialization, before other Kerberos routines are called; otherwise the routines which fetch the ticket cache file name may be called and return an undesired ticket file name until this routine is called. Because both functions rely on a file identified by name, there is a risk that an attacker may substitute an unexpected file that will be accessed via that name. For the system to be secure, one should guard against this possiblility.
APIs	**FunctionName** / **Comments** krb_recvauth krb_set_tkt_string
Method of Attack	The key issue with respect to TOCTOU vulnerabilities is that programs make assumptions about atomicity of actions. It is assumed that

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	checking the state or identity of a targeted resource followed by an action on that resource is all one action. In reality, there is a period of time between the check and the use that allows either an attacker to intentionally or another interleaved process or thread to unintentionally change the state of the targeted resource and yield unexpected and undesired results. If the attacker is able to (1) influence the file name that is used in the call or (2) alter the object referenced by the given file name to reference a different object or file, then the attacker could substitute different keys or ensure that keys are cached in a place that the attacker will have access to. In either case, the attacker will have knowledge of keys that should be secret, and so the cryptographic security of the sytem would be compromised.
Exception Criteria	
Solutions	

Solution Applicability	Solution Description	Solution Efficacy
When krb_recvauth() or krb_set_tkt_string() is used.	Do not allow untrusted parties to specify the filename to be passed to either of these functions. Ensure that the referenced file is secure from tampering by an untrusted party.	Effective.
Generally applicable.	The most basic advice for TOCTOU vulnerabilities is to not perform a check before the use. This does not resolve the underlying issue of the execution of a function on a resource whose state and identity cannot be assured, but it does help	Does not resolve the underlying vulnerability but limits the false sense of security given by the check.

		to limit the false sense of security given by the check.	
	Generally applicable.	Limit the interleaving of operations on files from multiple processes.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Limit the spread of time (cycles) between the check and use of a resource.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Recheck the resource after the use call to verify that the action was taken appropriately.	Checking the status after the operation does not change the fact that the operation may have been exploited but it does allow halting of the application in an error state to help limit further damage.

Signature Details	int krb_recvauth(const long options, const int fd, KTEXT ktext, const char *service, char *inst, const struct sockaddr_in *faddr, const struct sockaddr_in *laddr, AUTH_DAT *auth_data, const char *filename, Key_schedule schedule, char *version); void krb_set_tkt_string(const char *filename);
Examples of Incorrect Code	`krb_set_tkt_string("fileReadableByWorld");`
Examples of Corrected Code	`krb_set_tkt_string("fileWithPermissionsThatE`
Source References	• ITS4 Source Code Vulnerability Scanning Tool [2] • http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/ucd-ecs-95-09.pdf [3]

Recommended Resources	• man page for krb_recv_auth and related functions[4] • man page for krb_recv_auth and related functions[5]
Discriminant Set	**Operating System**: • Any **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com